CHAPTER Ins 3700 STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION

Statutory Authority: RSA 400-A:15, I.

PART Ins 3701 STANDARDS

Ins 3701.01 Purpose and scope.

(a) This rule establishes standards for developing and implementing administrative, technical and physical safeguards to protect the security, confidentiality and integrity of customer information, pursuant to Sections 501, 505(b), and 507 of the Gramm-Leach-Bliley Act, codified at 15 U.S.C. 6801, 6805(b) and 6807.

(b) Section 501(a) provides that it is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information. Section 501(b) requires the state insurance regulatory authorities to establish appropriate standards relating to administrative, technical and physical safeguards:

(1) To ensure the security and confidentiality of customer records and information;

(2) To protect against any anticipated threats of hazards to the security or integrity of such records; and

(3) To protect against unauthorized access to or use of records or information that could result in substantial harm or inconvenience to a customer.

(c) Section 505(b)(2) calls on state insurance regulatory authorities to implement the standards prescribed under Section 501(b) by rule with respect to persons engaged in providing insurance.

(d) Section 507 provides, among other things, that a state rule may afford persons greater privacy protections than those provided by subtitle A of Title V of the Gramm-Leach-Bliley Act. This rule requires that the safeguards established pursuant to this rule shall apply to nonpublic personal information, including nonpublic personal financial information and nonpublic personal health information.

Ins 3701.02 Definitions. For the purposes of this rule, the following definitions apply:

(a) "Customer" means a customer of the licensee as the term customer is defined in Ins 3001.04 (i).

(b) "Customer information" means nonpublic personal information as defined in Ins 3001.04 (s) about a customer, whether in paper, electronic or other form, that is maintained by or on behalf of the licensee.

(c) "Customer information systems" means the electronic or physical methods used to access, collect, store, use, transmit, protect or dispose of customer information.

(d) "Licensee" means a licensee as that term is defined in Ins 3001.04 (q), except that "licensee" shall not include: a purchasing group; or an unauthorized insurer in regard to the excess line business conducted pursuant to RSA 406-B.

(e) "Service provider" means a person that maintains, processes or otherwise is permitted access to customer information through its provision of services directly to the licensee.

Ins 3701.03 Information Security Program. Each licensee shall implement a comprehensive written information security program that includes administrative, technical and physical safeguards for the protection of customer information. The administrative, technical and physical safeguards included in the information security program shall be appropriate to the size and complexity of the licensee and the nature and scope of its activities.

Ins 3701.04 Objectives of Information Security Program. A licensee's information security program shall be designed to:

(a) Ensure the security and confidentiality of customer information;

(b) Protect against any anticipated threats or hazards to the security or integrity of the information; and

(c) Protect against unauthorized access to or use of the information that could result in substantial harm or inconvenience to any customer.

Ins 3701.05 Examples of Methods of Development and Implementation. The actions and procedures described in Ins 3701.06 through Ins 3701.09 are examples of methods of implementation of the requirements of Ins 3701.03 and Ins 3701.04. These examples are non-exclusive illustrations of actions and procedures that licensees may follow to implement Ins 3701.03 and Ins 3701.04.

Ins 3701.06 Assess Risk. The licensee:

(a) Identifies reasonably foreseeable internal or external threats that could result in unauthorized disclosure, misuse, alteration or destruction of customer information or customer information systems;

(b) Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information; and

(c) Assesses the sufficiency of policies, procedures, customer information systems and other safeguards in place to control risks.

Ins 3701.07 Manage and Control Risk. The licensee:

(a) Designs its information security program to control the identified risks, commensurate with the sensitivity of the information, as well as the complexity and scope of the licensee's activities;

(b) Trains staff, as appropriate, to implement the licensee's information security program; and

(c) Regularly tests or otherwise regularly monitors the key controls, systems and procedures of the information security program. The frequency and nature of these tests or other monitoring practices are determined by the licensee's risk assessment.

Ins 3701.08 Oversee Service Provider Arrangements. The licensee:

(a) Exercises appropriate due diligence in selecting its service providers; and

(b) Requires its service providers to implement appropriate measurers designed to meet the objectives of this rule, and, where indicated by the licensee's risk assessment, takes appropriate steps to confirm that its service providers have satisfied these obligations.

Ins 3701.09 Adjust the Program. The licensee monitors, evaluates and adjusts, as appropriate, the information security program in light of any relevant changes in technology, the sensitivity of its customer information, internal or external threats to information, and the licensee's own changing business

arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements and changes in customer information systems.

Ins 3701.10 Violations. Violations of any of the provisions of this part shall be subject to the penalties of RSA 400-A:15 III.

PART Ins 3702 CUSTOMER NOTICE

Statutory Authority: RSA 400-A:15, I.

Ins 3702.01 Purpose and Scope. This part establishes the standards for the notice to customers of a security breach involving the unauthorized access or use of the customer's information.

Ins 3702.02 Definitions. For the purposes of this part, definitions shall be the same as those delineated at Ins 3701.02 with the following exceptions:

(a) "Customer information" means nonpublic personal information as defined in RSA 359-C:19, IV. (a) and (b) about a customer, in electronic form, that is maintained by or on behalf of the licensee.

(b) "Unauthorized access to customer information" means the unauthorized acquisition of customer information that compromises the security, confidentiality or integrity of the customer information.

Ins 3702.03 Standards for Providing Notice.

(a) When a licensee becomes aware of an incident of unauthorized access to customer information, the licensee shall immediately conduct an investigation to promptly determine the likelihood that the information has been or will be misused.

(b) If a licensee determines that misuse of its customer information has occurred or is reasonably likely to occur or if a determination cannot be made, it shall notify the affected customer or customers and the department as soon as possible but not later than 30 days.

(c) Customer notice may be delayed if a law enforcement agency determines that notification will interfere with a criminal investigation and provides the licensee with a written request for the delay. However, the licensee shall notify its customer or customers pursuant to (b) above as soon as the law enforcement agency informs the licensee that notification will no longer interfere with the investigation.

Ins 3702.04 Affected Customers.

(a) If a licensee, based upon its investigation, can determine from its logs or other data precisely which customers' information has been improperly accessed, it may limit notification to those customers with regard to whom the licensee determines that misuse of their information has occurred or is reasonably possible.

(b) If the licensee is unable to identify which specific customers' information has been accessed, it shall notify all customers by substitute notice in accordance with RSA 359-C:20 III. (d).

Ins 3702.05 Content of Customer Notice.

(a) Customer notice shall be given in a clear and conspicuous manner. The notice shall describe the incident in general terms, the type of customer information that was the subject of the unauthorized access or use and the approximate date of the breach.

(b) The notice shall include a telephone number that customers may call for further information and assistance.

(c) Additionally, insurers may include in their notice the following information:

(1) A general description of what the licensee has done to protect the customers' information from further unauthorized access;

(2) A reminder to customers of the need to remain vigilant over the next year or two to promptly report incidents of suspected identify theft to the licensee and the appropriate authorities;

(3) A recommendation that the customer review bank and creditor statements and immediately report any suspicious activity to the appropriate authorities;

(4) A description of fraud alerts and an explanation of how the customer may place a fraud alert in the customer's consumer reports to put the customer's creditors on notice that the customer may be a victim of fraud;

(5) A recommendation that the customer periodically obtain credit reports from each nationwide credit reporting agency and have information relating to fraudulent transactions deleted; and

(6) An explanation of how the customer may obtain a credit report free of charge.

Ins 3702.06 Delivery of Customer Notice.

(a) Customer notice shall be delivered in any manner designed to ensure that a customer can be expected to receive it. The licensee may choose to contact all customers affected by telephone provided the licensee maintains a log of each such notification, or by U.S. mail, or by electronic mail if the customer has agreed to receive communications electronically.

Ins 3702.07 Violations. Knowing violations of any of the provisions of this part shall be subject to the penalties of RSA 400-A:15 III.

(ins3700adopted061107)